The General Data Protection Regulation (GDPR) and Subject Access Requests

This month's Spotlight focuses on how individuals can access their data through a subject access request under the new General Data Protection Regulation.

The current law – Data Protection Act 1998

Currently, the rights of subject access in Europe are defined by the EC Data Protection Directive (95/46/EC). In the UK, the Data Protection Act 1998 (DPA) gives effect to the Directive where s7 of the DPA applies on making a subject access request.

A subject access request is a written request made by an individual to see information about themselves that an organisation holds. However, the right of access goes further than this and an individual who makes a written request is entitled to be:

- told whether any personal data is being processed
- given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people
- given a copy of the information comprising the data and given details of the source of the data (where this is available)

There is no particular form for making a request, and it does not have to include the words 'subject access' or make any reference to the DPA. It is enough for the person making the request to demand to be told what information is held about them. You can also use this template letter.

Organisations must respond to any requests that are made in writing, including those by email, fax, and social media – such as Facebook and Twitter.

The cost to make a subject access request

The maximum fee that can be charged to release personal data is £10. The individual cannot be charged more than this unless the request is for health records, in which case up to £50 can be charged.

The time limit to comply with the request

The organisation must comply 'promptly' and in any case within 40 calendar days of receiving the request. However, the 40 days does not start until the £10 fee has been paid.

An organisation cannot ignore a request just because the fee has not been paid. In that case they should contact the individual and let them know payment is required.

GDPR

However, the DPA will be replaced by the General Data Protection Regulation (EU) 2016/679 (GDPR) and will apply from **25 May 2018**. The GDPR has been designed to harmonise data privacy laws across Europe, to protect and empower all EU citizens data privacy and to reshape the way organizations across the region approach data privacy. The government has confirmed that the commencement of the GDPR will not be affected by the UK's decision to leave the EU.

As with the DPA, the GDPR applies to 'personal data', but the GDPR's definition is more detailed and the definition now includes 'an online identifier', such as IP address as an example of personal data (Article 4(1)).

Right of access

Similar to the DPA, individuals will still be able to access their personal data by making a subject access request, and Article 15 GPDR goes through privacy information that must be provided to an individual (privacy notice).

GDPR Recital (paragraph) 63 states that the purpose of allowing individuals to access their personal data is 'to be aware of, and verify, the lawfulness of the processing'.

When the GDPR applies from 25 May, the ICO will update the template – referring to the right under the GDPR to have free access to personal data.

The cost to make a subject access request

The organisation must provide the information **free of charge**.

However, if an organisation feels that a request is 'manifestly unfounded or excessive, particularly if it is repetitive', a reasonable fee can be charged, or the organisation can refuse to act on the request (Article 12(5) GDPR).

What counts as a 'reasonable' fee is not defined in the GDPR. It is worth noting that the organisation would need to demonstrate the manifestly unfounded or excessive character of the request.

The time limit to comply with the request

The organisation must comply without 'undue delay' and in any event within **one month** of receipt of the request (Article 12 GDPR).

However, that period may be extended by two further months where necessary, 'taking into account the complexity and number of the requests'. The individual would need to be informed of any extension within one month of receipt of the request, and also explaining reasons for the delay (Article 12(3) GDPR).

Using a subject access request

Advisers sometimes see clients who don't have enough documentation to provide a full picture of their circumstances.

My client's credit agreement is regulated by the Consumer Credit Act 1974 (CCA) and so a copy of the credit agreement can be requested under Section 77. Do I still need to make a subject access request?

In the majority of cases, you shouldn't need to make a subject access request if all you are requesting is the credit agreement, which costs £1. If more information is needed, such as statements of account or ensuring the creditor has provided all of the required CCA notices, making a subject access request would ensure documents are not provided piecemeal, and also ensures the creditor responds within a certain time limit.

I believe a debt may be statute barred, as it has been more than six years without acknowledging the debt. However, the creditor says a payment was made within the six years, but has not provided a statement of account. Would making a subject access request in this situation restart the limitation period?

No. As long as there is no reference to 'debt', making the subject access request will not count as an acknowledgment.

Further information

DPA

In general, the ICO has a Code of Practice that organisations should use to comply with the DPA. Principle 6 in particular focuses on subject access rights. The ICO has also published guidance on the subject for organisations.

GDPR

See the ICO 'Guide to the GDPR' and an 'Overview of the GDPR' to learn more about the GDPR in general. You can also contact the ICO's recently created SME GDPR helpline on 0303 123 1113.